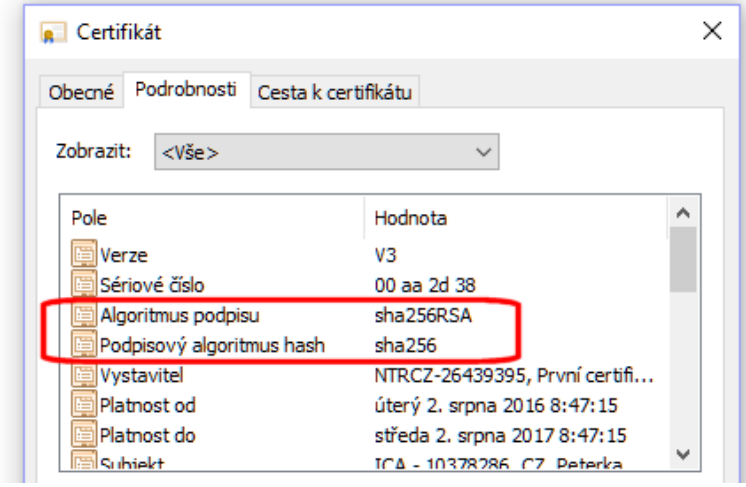
Testovací dokument

Cílem tohoto dokumentu je ukázat, že volba hashovací funkce při (každém jednotlivém) podepisování konkrétního dokumentu je nezávislá na hashovací funkci, (jednorázově) použité při vydání podpisového certifikátu.

Tento PDF dokument má pět kvalifikovaných elektronických podpisů v referenčním formátu PAdES Baseline-LT. Všechny jsou založeny na stejném kvalifikovaném certifikátu, při jehož vydání byla využita hashovací funkce SHA256 (pro otisk té části certifikátu, kterou její vydavatel opatřil svým podpisem, resp. značkou).



Každý z pěti podpisů tohoto dokumentu ale pro samotné podepsání (pro vytvoření otisku/hashe podepisovaného dokumentu) využívá jinou hashovací funkci, resp. jinou její variantu:

hashovací funkce	vizualizovaný podpis
MD5	RNDr. Ing. Jiří Peterka Digitálně podepsal RNDr. Ing. Jiří Peterka Datum: 2017.02.24 21:42:17 +01'00'
SHA1	RNDr. Ing. Jiří Peterka Digitálně podepsal RNDr. Ing. Jiří Peterka Datum: 2017.02.24 21:58:26 +01'00'
SHA256	RNDr. Ing. Jiří Peterka Digitálně podepsal RNDr. Ing. Jiří Peterka Datum: 2017.02.24 22:18:09 +01'00'
SHA384	RNDr. Ing. Jiří Peterka Digitálně podepsal RNDr. Ing. Jiří Peterka Datum: 2017.02.24 22:24:13 +01'00'
SHA512	RNDr. Ing. Jiří Peterka Digitálně podepsal RNDr. Ing. Jiří Peterka Datum: 2017.02.24 22:26:22 +01'00'

To, která hashovací funkce byla pro konkrétní podpis využita, lze ověřit například v programu Adobe Acrobat Reader DC přes „Vlastnosti podpisu“ a pak „Další vlastnosti podpisu“, viz následující obrázek: